RubénS

PRÁCTICA 4 UD 1: Footprinting y enumeración con DNS

Objetivos: conocer las técnicas de footprinting de DNS para recopilar información sobre el dominio y los hosts que posee una organización.
DESCARGO DE RESPONSABILIDAD: el equipo docente y el centro no se hacen responsables del mal uso que pueda realizar el alumno con las técnicas aprendidas en la realización de esta práctica.

Introducción

El objetivo de esta práctica es que el alumno utilice la información de una fuente pública como es **DNS** para descubrir los hosts de un dominio. Este tipo de técnicas entran también en la fase de enumeración.
Se utilizarán para ello herramientas como **fierce**, **dnsenum**, **theHarvester**, **dnsrecon** o **dnsdumpster**.

1. Fierce

Utiliza la herramienta fierce para obtener información sobre el dominio utilizando un ataque por diccionario.
Puedes consultar la ayuda con fierce --help.
Con fierce no puedes cambiar los servidores dns a los que realizar las consultas, por tanto usa los del sistema. Si miras en la ayuda, la opción -dns-servers es la que te permite usar otro dns pero para hacer las consultas inversas. Por tanto, si quieres que te funcione fierce realizando un ataque a un dominio ficticio que tienes en un servidor dns, debes cambiar provisionalmente los servidores dns de kali. Lo puedes hacer editando como root el /etc/resolv.conf y cambiando la directiva nameserver o bien modificando los ajustes IPv4 de las propiedades de la conexión de Kali poniéndola a "Solo direcciones DHCP" y estableciendo como dns, la dirección IP del servidor que vas a atacar.
Lo primero es Instalar Fierce (si no está instalado) con sudo apt install fierce.
Que opciones admite Fierce según la ayuda:

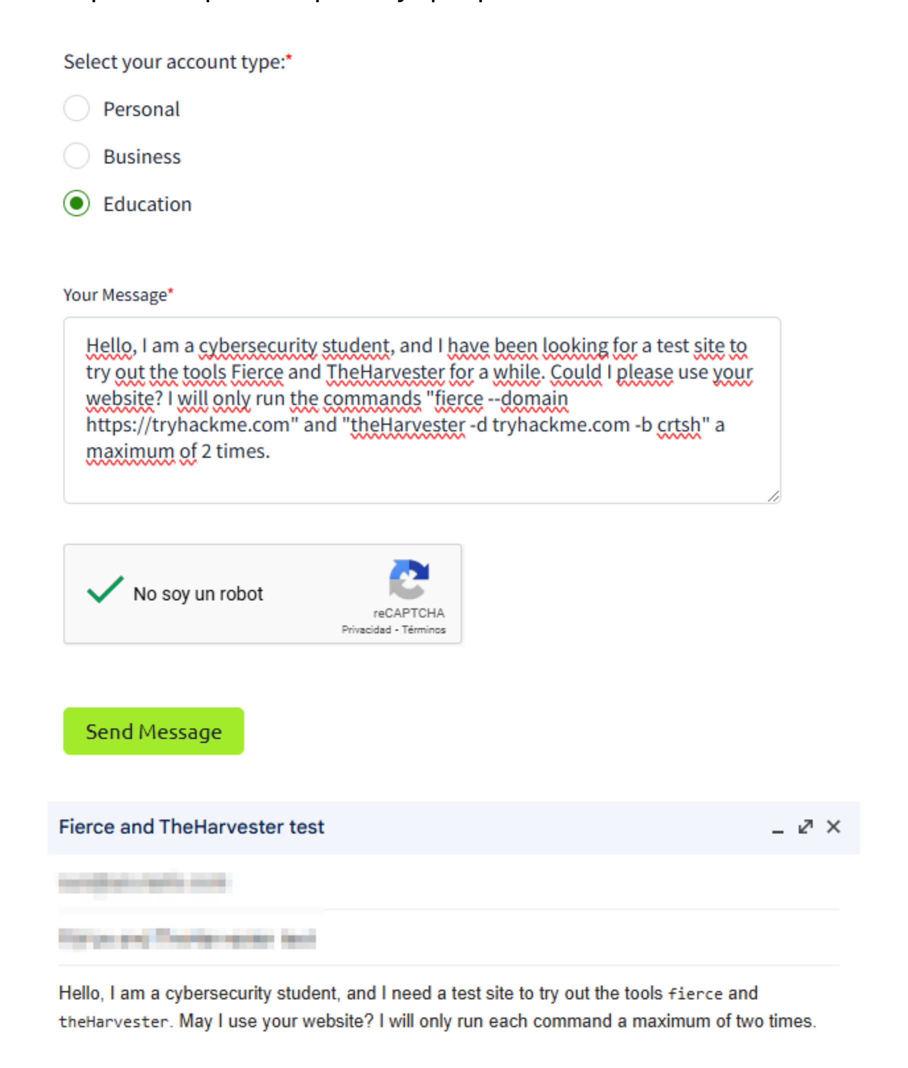
```
┌──(kali㉿kali)-[~]
└─$ fierce --help
usage: fierce [-h] [--domain DOMAIN] [--connect] [--wide]
              [--traverse TRAVERSE] [--search SEARCH [SEARCH ...]]
              [--range RANGE] [--delay DELAY]
              [--subdomains SUBDOMAINS [SUBDOMAINS ...] | --subdomain-file
              SUBDOMAIN_FILE] [--dns-servers DNS_SERVERS [DNS_SERVERS ...]
              | --dns-file DNS_FILE] [--tcp]

        A DNS reconnaissance tool for locating non-contiguous IP space.
```

Voy a probar primero que información se muestra usando como ejemplo una **web real que está hecha para ser atacada** y luego **probaré una ficticia local**. Antes de realizar análisis de seguridad de cualquier dominio necesito autorización para no cometer una ilegalidad. Voy a usar vulnweb.com, que es una plataforma diseñada para pruebas de hackers y no tiene información crítica. Aunque se puede demostrar que se ha hecho con un propósito educativo y sin mala intención y que el nombre o razón de ser de la web puede dar lugar a confusión, si no se pide autorización siempre existe riesgo de tener problemas.

Advertencia : Esta no es una tienda real. Es una aplicación PHP de ejemplo, que es vulnerable a ataques web. Su objetivo es ayudarle a probar Acunetix. También le ayuda a entender cómo los errores de los desarrolladores y las configuraciones incorrectas pueden permitir que alguien entre en su sitio web. Puede utilizarla para probar otras herramientas y también sus habilidades de piratería manual. Consejo: Busque posibles inyecciones SQL, secuencias de comandos entre sitios (XSS) y falsificación de solicitudes entre sitios (CSRF), entre otros.

Es por ello que siempre hay que pedir autorización:



Como quiero obtener información sobre http://testphp.vulnweb.com/ es aconsejable dirigir las consultas a los servidores DNS autoritativos.
Los DNS de Google (8.8.8.8) son generales y pueden no tener la información más reciente o detallada.

Modifico el archivo /etc/resolv.conf para incluir los DNS de Google y ver la diferencia:

```
kali@kali: ~
File  Actions  Edit  View  Help
  GNU nano 8.1                        /etc/resolv.conf *
# Generated by NetworkManager
nameserver 8.8.8.8
nameserver 8.8.4.4
```

Para consultar el dominio http://testphp.vulnweb.com/ ejecuto:

```
┌──(kali㉿kali)-[~]
└─$ fierce --domain https://testphp.vulnweb.com
NS: ns4.eurodns.com. ns3.eurodns.com. ns2.eurodns.com. ns1.eurodns.com.
SOA: ns1.eurodns.com. (199.167.66.107)
Zone: failure
Wildcard: 44.228.249.3
^CExiting...
```

Si quisiera especificar unos servidores DNS concretos sin tener que editar el archivo /etc/resolv.conf puedo usar la opción --dns-servers.

Voy a ver los DNS que usa esa web:

```
┌──(kali㉿kali)-[~]
└─$ dig NS vulnweb.com

; <<>> DiG 9.20.0-Debian <<>> NS vulnweb.com
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 31926
;; flags: qr rd ra; QUERY: 1, ANSWER: 4, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 512
;; QUESTION SECTION:
;vulnweb.com.                   IN      NS

;; ANSWER SECTION:
vulnweb.com.            21527   IN      NS      ns4.eurodns.com.
vulnweb.com.            21527   IN      NS      ns2.eurodns.com.
vulnweb.com.            21527   IN      NS      ns1.eurodns.com.
vulnweb.com.            21527   IN      NS      ns3.eurodns.com.

;; Query time: 16 msec
;; SERVER: 8.8.8.8#53(8.8.8.8) (UDP)
;; WHEN: Sat Dec 07 08:52:46 EST 2024
;; MSG SIZE  rcvd: 120


┌──(kali㉿kali)-[~]
└─$ dig +short ns1.eurodns.com
199.167.66.107
```

Apunto a los DNS que me ha dado el comando DIG:

```
┌──(kali㉿kali)-[~]
└─$ fierce --domain testphp.vulnweb.com --dns-servers 199.167.66.107
NS: ns1.eurodns.com. ns2.eurodns.com. ns3.eurodns.com. ns4.eurodns.com.
SOA: ns1.eurodns.com. (199.167.66.107)
Zone: failure
Wildcard: failure
```

Pruebo con mmebvba usando los DNS de Google, ya que no hay diferencia:

```
┌──(kali㉿kali)-[~]
└─$ fierce --domain [redacted].com
NS: ns4[redacted]domaincontrol.com. ns46.domaincontrol.com.
SOA: ns4[redacted].domaincontrol.com. (97.[redacted].102.23)
Zone: failure
Wildcard: failure
Found: downloads.[redacted]com. (81.1[redacted].172.83)
Nearby:
{'81.16[redacted].172.7[redacted]': 'd51a[redacted]ac4e.access.telenet.be.',
 '81.16[redacted].172.7[redacted]': 'd51a[redacted]ac4f.access.telenet.be.',
 '81.16[redacted].172.8[redacted]': 'd51a[redacted]ac50.access.telenet.be.',
 '81.16[redacted].172.8[redacted]': 'd51a[redacted]ac51.access.telenet.be.',
 '81.16[redacted].172.8[redacted]': 'd51a[redacted]ac52.access.telenet.be.',
 '81.16[redacted].172.8[redacted]': 'd51a[redacted]ac53.access.telenet.be.',
 '81.16[redacted].172.8[redacted]': 'd51a[redacted]ac54.access.telenet.be.',
 '81.16[redacted].172.8[redacted]': 'd51a[redacted]ac55.access.telenet.be.',
 '81.16[redacted].172.8[redacted]': 'd51a[redacted]ac56.access.telenet.be.',
 '81.16[redacted].172.8[redacted]': 'd51a[redacted]ac57.access.telenet.be.',
 '81.16[redacted].172.8[redacted]': 'd51a[redacted]ac58.access.telenet.be.'}
```

NS (servidores de nombres): ns4x.domaincontrol.com y ns4x.domaincontrol.com.

SOA (Start of Authority): ns45.domaincontrol.com con dirección IP 97.7x.102.23

- **Zone: failure** indica que los servidores DNS están configurados para denegar solicitudes de transferencia de zona
- **Wildcard: failure** significa que no hay un registro wildcard (*) configurado en el dominio.

La herramienta identificó un subdominio y sus direccion IP:

  - downloads.xxxxxx.com → 81.1x5.172.83

Direcciones IP cercanas detectadas (Nearby):

81.1x5.172.78: d51a5ac4e.access.telenet.be

Para realizar el mismo ejercicio pero en una web **ficticia** primero tenemos que hacer lo siguiente:

Instalo bind9, que es un servidor DNS:

```
┌──(kali㉿kali)-[~]
└─$ sudo apt install bind9

[sudo] password for kali:
Upgrading:
  bind9-dnsutils  bind9-host  bind9-libs

Installing:
  bind9

Installing dependencies:
  bind9-utils

Suggested packages:
  bind-doc  resolvconf  ufw
```

Edito el fichero de configuración de zonas /etc/bind/named.conf.local

```
  GNU nano 8.1                 /etc/bind/named.conf.local
//
// Do any local configuration here
//

// Consider adding the 1918 zones here, if they are not used in your
// organization
//include "/etc/bind/zones.rfc1918";

zone "domirub.local" {
    type master;
    file "/etc/bind/db.domirub.local";
};

zone "0.168.192.in-addr.arpa" {
    type master;
    file "/etc/bind/db.192.168.0.rev";
};
```

Crea el archivo de zona directa para el dominio:

```
  GNU nano 8.1                          /etc/bind/db.domirub.local
$TTL 604800
@ IN SOA domirub.local. root.domirub.local. (
    2024010100 ; Serial
    604800     ; Refresh
    86400      ; Retry
    2419200    ; Expire
    604800 )   ; Negative Cache TTL
;
@ IN NS ns1.domirub.local.
@ IN A 192.168.0.1

ns1     IN A 192.168.0.1
web     IN A 192.168.0.10
mail    IN A 192.168.0.20
ftp     IN A 192.168.0.30
```

Creo la zona inversa:

```
  GNU nano 8.1                          /etc/bind/db.192.168.0.rev *
$TTL 604800
@ IN SOA domirub.local. root.domirub.local. (
    2024010100 ; Serial
    604800     ; Refresh
    86400      ; Retry
    2419200    ; Expire
    604800 )   ; Negative Cache TTL
;
@ IN NS ns1.domirub.local.

1  IN PTR ns1.domirub.local.
10 IN PTR web.domirub.local.
20 IN PTR mail.domirub.local.
30 IN PTR ftp.domirub.local.
```

Doy permisos al archivo, reinicio el servicio Bind9 y modifico la configuración de la red para apuntar al servidor DNS local:

```
xubu@rubensVM:~$ sudo chown bind:bind /etc/bind/db.*
xubu@rubensVM:~$ sudo systemctl restart bind9
```

Compruebo que la información es correcta en /etc/resolv.conf:

```
  GNU nano 8.1                              /etc/resolv.conf
# This is /run/systemd/resolve/stub-resolv.conf managed by man:systemd-resolved(8).
# Do not edit.
#
# This file might be symlinked as /etc/resolv.conf. If you're looking at
# /etc/resolv.conf and seeing this text, you have followed the symlink.
#
# This is a dynamic resolv.conf file for connecting local clients to the
# internal DNS stub resolver of systemd-resolved. This file lists all
# configured search domains.
#
# Run "resolvectl status" to see details about the uplink DNS servers
# currently in use.
#
# Third party programs should typically not access this file directly, but only
# through the symlink at /etc/resolv.conf. To manage man:resolv.conf(5) in a
# different way, replace this symlink by a static file or a different symlink.
#
# See man:systemd-resolved.service(8) for details about the supported modes of
# operation for /etc/resolv.conf.

nameserver 127.0.0.53
options edns0 trust-ad
search Home
```

No he editado directamente este archivo porque en este caso está generado automáticamente por NetworkManager y se cambia cada vez que se reinicia el servicio.

Se podría solucionar de muchas formas, la más fácil es poner el DNS a través de la interfaz de NetworkManger, sin embargo, en su lugar optaré por especificar el dns en el comando Fierce para no tener que cambiar el DNS en cada prueba.

Compruebo que la zona está correctamente creada:

```
xubu@rubensVM:~$ sudo named-checkzone domirub.local /etc/bind/db.domirub.local
zone domirub.local/IN: loaded serial 2024010100
OK
xubu@rubensVM:~$
```

Al usar la herramienta Fierce saca el NS y SOA, pero obtengo este error:

```
xubu@rubensVM:~$ fierce --domain domirub.local --dns-servers 127.0.0.1
NS: ns1.domirub.local.
SOA: domirub.local. (192.168.0.1)
Zone: failure
Traceback (most recent call last):
  File "/usr/bin/fierce", line 33, in <module>
    sys.exit(load_entry_point('fierce==1.5.0', 'console_scripts', 'fierce')())
             ^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^

  File "/usr/lib/python3/dist-packages/fierce/fierce.py", line 491, in main
    fierce(**vars(args))
  File "/usr/lib/python3/dist-packages/fierce/fierce.py", line 334, in fierce
    random_subdomain = str(random.randint(1e10, 1e11))  # noqa DUO102, non-crypto
use
                           ^^^^^^^^^^^^^^^^^^^^^^^^^^^^

  File "/usr/lib/python3.12/random.py", line 336, in randint
    return self.randrange(a, b+1)
           ^^^^^^^^^^^^^^^^^^^^^^

  File "/usr/lib/python3.12/random.py", line 301, in randrange
    istart = _index(start)
             ^^^^^^^^^^^^^

TypeError: 'float' object cannot be interpreted as an integer
xubu@rubensVM:~$
```

Compruebo que puedo hacer un dig y la información es correcta, por lo que el problema está en el código de Fierce.

```
xubu@rubensVM:~$ dig domirub.local NS SOA
;; Warning, extra type option

; <<>> DiG 9.20.0-2ubuntu3-Ubuntu <<>> domirub.local NS SOA
;; global options: +cmd
;; Got answer:
;; WARNING: .local is reserved for Multicast DNS
;; You are currently testing what happens when an mDNS query is leaked to DNS
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 38265
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 1232
; COOKIE: 6f5e6211fcb8307d010000006755b6169140791036ab3bdb (good)
;; QUESTION SECTION:
;domirub.local.                 IN      SOA

;; ANSWER SECTION:
domirub.local.          604800  IN      SOA     domirub.local. root.domirub.local. 2024010100 604800 86400 2419200 604800

;; Query time: 1 msec
;; SERVER: 127.0.0.1#53(127.0.0.1) (UDP)
;; WHEN: Sun Dec 08 16:07:02 CET 2024
;; MSG SIZE  rcvd: 111

xubu@rubensVM:~$ dig domirub.local NS

; <<>> DiG 9.20.0-2ubuntu3-Ubuntu <<>> domirub.local NS
;; global options: +cmd
;; Got answer:
;; WARNING: .local is reserved for Multicast DNS
;; You are currently testing what happens when an mDNS query is leaked to DNS
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 50779
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 2

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 1232
; COOKIE: 65480da020adb4ee010000006755b6212c329a2e7d5904c3 (good)
;; QUESTION SECTION:
;domirub.local.                 IN      NS

;; ANSWER SECTION:
domirub.local.          604800  IN      NS      ns1.domirub.local.

;; ADDITIONAL SECTION:
ns1.domirub.local.      604800  IN      A       192.168.0.1

;; Query time: 2 msec
;; SERVER: 127.0.0.1#53(127.0.0.1) (UDP)
;; WHEN: Sun Dec 08 16:07:13 CET 2024
;; MSG SIZE  rcvd: 104
```

2. Dnsrecon

Desde la consola de Kali linux, utiliza la herramientas dnsrecon para obtener información sobre el dominio que has creado en el ejercicio 1 utilizando un ataque por diccionario.
Puedes consultar la ayuda con dnsrecon --help.
La opción -n es la que te permite usar tu propio dns para hacer las consultas, y no los servidores dns de internet.
Busca la opción en la ayuda, que te permite especificar el tipo de enumeración a fuerza bruta.
Dnsrecon permite, entre otras, usar enumeración con motores de búsqueda como Bing,Yandex. En nuestro caso como es un dominio que no existe en Internet, debemos hacerlo con fuerza bruta con un diccionario de palabras.
Dnsrecon usa su diccionario de palabras (/usr/share/dnsrecon/namelist.txt) pero puedes indicarle uno. Realiza el ataque primero sin indicar diccionario y después con un fichero de palabras de tu creación (o puedes buscarlo de Internet) y compara los resultados.
Ejecuta ahora de nuevo el ataque de fuerza bruta pero guarda los resultados en ficheros de tipo CSV, XML o JSON (es mejor indicar la ruta absoluta del nombre del fichero a usar porque sino produce un error de permisos en la creación del archivo) Por defecto fierce usa su diccionario de palabras pero puedes indicarle uno. Realiza el ataque primero sin indicar diccionario y después con un fichero de palabras de tu creación (o puedes buscarlo de Internet) y compara los resultados.
Una vez finalizado el ejercicio, deja el fichero /etc/resolv.conf como estaba inicialmente.

-d: Especifica el dominio.
-n: Especifica el servidor DNS (127.0.0.1 en este caso).
-t brt: Realiza una enumeraciÓn a fuerza bruta para descubrir subdominios.
Este comando usa el diccionario predeterminado de dnsrecon (/usr/share/dnsrecon/namelist.txt).

Usando el diccionario por defecto:

```
xubu@rubensVM:~$ dnsrecon -d ficticio.local -n 127.0.0.1 -t brt
[*] No dictionary file has been specified.
[*] Using the dictionary file: /usr/share/dnsrecon/dnsrecon/data/namelist.txt (provided by tool)
[*] brt: Performing host and subdomain brute force against ficticio.local...
[+] 0 Records Found
```

Creando un diccionario:

```
  GNU nano 8.1   /home/xubu/domirub_diccionario.txt
ns1
web
mail
ftp
```

Usando el diccionario creado y guardando los resultados en un json:

```
xubu@rubensVM:~$ dnsrecon -d domirub.local -n 127.0.0.1 -t brt -D ~/domirub_diccionario.txt -c ~/resultados.json
[*] Using the dictionary file: /home/xubu/domirub_diccionario.txt (provided by user)
[*] brt: Performing host and subdomain brute force against domirub.local...
[+]      A ns1.domirub.local 192.168.0.1
[+]      A mail.domirub.local 192.168.0.20
[+]      A ftp.domirub.local 192.168.0.30
[+]      A web.domirub.local 192.168.0.10
[+] 4 Records Found
[*] Saving records to CSV file: /home/xubu/resultados.json
```

3. Dnsenum

Desde la consola de kali linux, utiliza la herramientas dnsenum para obtener información sobre el utilizando un ataque por diccionario.
Puedes consultar la ayuda con dnsenum --help.
La opción --dnsserver es la que te permite usar tu propio DNS para hacer las consultas, y no los servidores DNS de internet.
Realiza el ataque primero sin indicar diccionario (se usa /usr/share/dnsenum/dns.txt: por defecto) y después con un fichero de palabras de tu creación (o puedes buscarlo de Internet) y compara los resultados.

--dnsserver: Sirve para usar tu propio servidor DNS.

Ataque sin diccionario:

```
xubu@rubensVM:~$ dnsenum domirub.local --dnsserver 127.0.0.1
dnsenum VERSION:1.3.1

-----   domirub.local   -----


Host's addresses:
__________________

domirub.local.                           604800   IN    A        192.168.0.1


Name Servers:
______________

ns1.domirub.local.                       604800   IN    A        192.168.0.1


Mail (MX) Servers:
___________________



Trying Zone Transfers and getting Bind Versions:
_________________________________________________


Trying Zone Transfer for domirub.local on ns1.domirub.local ...
AXFR record query failed: Connection timed out


Brute forcing with /usr/share/dnsenum/dns.txt:
_______________________________________________

ftp.domirub.local.                       604800   IN    A        192.168.0.30
mail.domirub.local.                      604800   IN    A        192.168.0.20
ns1.domirub.local.                       604800   IN    A        192.168.0.1
web.domirub.local.                       604800   IN    A        192.168.0.10


domirub.local class C netranges:
_________________________________



Performing reverse lookup on 0 ip addresses:
_____________________________________________


0 results out of 0 IP addresses.


domirub.local ip blocks:
_________________________


done.
```

Creando un diccionario:

```
  GNU nano 8.1 /home/xubu/mi_diccionario_dnsenum.txt *
ns1
web
mail
ftp
```

Ataque con diccionario con el comando dnsrecon -d domirub.local -n 127.0.0.1 -t brt -D ~/domirub_diccionario.txt:

```
xubu@rubensVM:~$ dnsrecon -d domirub.local -n 127.0.0.1 -t brt -D ~/domirub_diccionario.txt
[*] Using the dictionary file: /home/xubu/domirub_diccionario.txt (provided by user)
[*] brt: Performing host and subdomain brute force against domirub.local...
[+]      A ns1.domirub.local 192.168.0.1
[+]      A web.domirub.local 192.168.0.10
[+]      A ftp.domirub.local 192.168.0.30
[+]      A mail.domirub.local 192.168.0.20
[+] 4 Records Found
```

Este comando hace un ataque de fuerza bruta (-t brt) contra el dominio domirub.local utilizando el servidor DNS local (-n 127.0.0.1) y un diccionario personalizado (-D ~/domirub_diccionario.txt).

El ataque normal con dnsenum utiliza su diccionario por defecto (/usr/share/dnsenum/dns.txt).
Este diccionario ya contiene palabras genéricas como ftp, mail, www, etc., que coinciden con los registros configurados en mi servidor.

4. TheHarvester

theHarvester es una potente herramienta de OSINT que usando fuentes públicas como buscadores, dns, redes sociales, etc es capaz de automatizar la búsqueda de personas o usuarios de la organización, nombres de hosts, direcciones de correo etc.

Desde la consola de kali linux, utiliza la herramientas theHarvester para obtener información sobre el dominio utilizando un ataque por diccionario.
Puedes consultar la ayuda con theHarvester --help.
Consulta la opción que te permite usar sólo la función de búsqueda dns por fuerza
bruta, que es la que vamos a usar. Consulta también el parámetro que te permite usar tu propio dns para hacer las consultas, y no los servidores dns de internet.
A continuación realiza el ataque de reconocimiento contra el dominio y el servidor.

Instalación: https://github.com/laramies/theHarvester/wiki/Installation

-b dns: Selecciona el modo de búsqueda DNS.
-c: Usa un servidor DNS personalizado.
-f: Especifica un archivo de diccionario para fuerza bruta.
-d: Especifica el dominio objetivo.

```
python3 theHarvester.py -d domirub.local -e 127.0.0.1 --dns-brute -f ~/mi_diccionario.txt > resultados.txt
```

El comando genera una lista con muchos subdominios que no existen, como parte del ataque de fuerza bruta:

```
ftp3.domirub.local:
www.marketing.domirub.local:
ns101.domirub.local:
automotive.domirub.local:
tomcat.domirub.local:
counter.domirub.local:
www.eu.domirub.local:
autoconfig.travel.domirub.local:
apache.domirub.local:

[*] Reporting started.
[*] XML File saved.
[*] JSON File saved.
```

Voy a probar a buscar información de una web publicada en internet a la que es legal atacar, en este caso vulnweb.com en Bing, ya que tiene más sentido:

```
┌──(kali㉿kali)-[~]
└─$ theHarvester -d vulnweb.com -b bing

Read proxies.yaml from /home/kali/.theHarvester/proxies.yaml
*******************************************************************
*  _   _                                            _             *
* | |_| |__   ___    /\  /\__ _ _ ____   _____  ___| |_ ___ _ __  *
* | __|  _ \ / _ \  / /_/ / _` | '__\ \ / / _ \/ __| __/ _ \ '__| *
* | |_| | | |  __/ / __  / (_| | |   \ V /  __/\__ \ ||  __/ |    *
*  \__|_| |_|\___| \/ /_/ \__,_|_|    \_/ \___||___/\__\___|_|    *
*                                                                 *
* theHarvester 4.6.0                                              *
* Coded by Christian Martorella                                   *
* Edge-Security Research                                          *
* cmartorella@edge-security.com                                   *
*                                                                 *
*******************************************************************

[*] Target: vulnweb.com

Created default api-keys.yaml at /home/kali/.theHarvester/api-keys.yaml
        Searching 0 results.
[*] Searching Bing.

[*] No IPs found.

[*] No emails found.

[*] Hosts found: 14
---------------------
252Ftestphp.vulnweb.com
2Ftestphp.vulnweb.com
Testphp.vulnweb.com
estphp.vulnweb.com
localhost.vulnweb.com
rest.vulnweb.com
scan-report-testphp.vulnweb.com
testap.vulnweb.com
testasp.vulnweb.com
testaspnet.vulnweb.com
testhtml5.vulnweb.com
testoho.vulnweb.com
testphp.vulnweb.com
testpphp.vulnweb.com
```

Para hacer una búsqueda más exhaustiva, theHarvester -d vulnweb.com -b all

```
└─$ theHarvester -d vulnweb.com -b all
```

Para la mayoría de cosas me faltan as API key. Muestro esto para que se vea la cantidad de recursos que usa en sus búsquedas:

```
Read api-keys.yaml from /home/kali/.theHarvester/api-keys.yaml

[!] Missing API key for bevigil.
Read api-keys.yaml from /home/kali/.theHarvester/api-keys.yaml

[!] Missing API key for binaryedge.
Read api-keys.yaml from /home/kali/.theHarvester/api-keys.yaml
Read api-keys.yaml from /home/kali/.theHarvester/api-keys.yaml
Read api-keys.yaml from /home/kali/.theHarvester/api-keys.yaml

[!] Missing API key for bufferoverun.
Read api-keys.yaml from /home/kali/.theHarvester/api-keys.yaml
Read api-keys.yaml from /home/kali/.theHarvester/api-keys.yaml

[!] Missing API key for Censys ID and/or Secret.
Read api-keys.yaml from /home/kali/.theHarvester/api-keys.yaml

[!] Missing API key for criminalip.
Read api-keys.yaml from /home/kali/.theHarvester/api-keys.yaml

[!] Missing API key for fullhunt.
Read api-keys.yaml from /home/kali/.theHarvester/api-keys.yaml

[!] Missing API key for Github.
Read api-keys.yaml from /home/kali/.theHarvester/api-keys.yaml

[!] Missing API key for Hunter.
Read api-keys.yaml from /home/kali/.theHarvester/api-keys.yaml

[!] Missing API key for hunterhow.
Read api-keys.yaml from /home/kali/.theHarvester/api-keys.yaml

[!] Missing API key for Intelx.
Read api-keys.yaml from /home/kali/.theHarvester/api-keys.yaml

[!] Missing API key for netlas.
Read api-keys.yaml from /home/kali/.theHarvester/api-keys.yaml

[!] Missing API key for onyphe.
Read api-keys.yaml from /home/kali/.theHarvester/api-keys.yaml

[!] Missing API key for PentestTools.
Read api-keys.yaml from /home/kali/.theHarvester/api-keys.yaml

[!] Missing API key for ProjectDiscovery.
Read api-keys.yaml from /home/kali/.theHarvester/api-keys.yaml

[!] Missing API key for RocketReach.
Read api-keys.yaml from /home/kali/.theHarvester/api-keys.yaml

[!] Missing API key for Securitytrail.
Read api-keys.yaml from /home/kali/.theHarvester/api-keys.yaml
Read api-keys.yaml from /home/kali/.theHarvester/api-keys.yaml
```

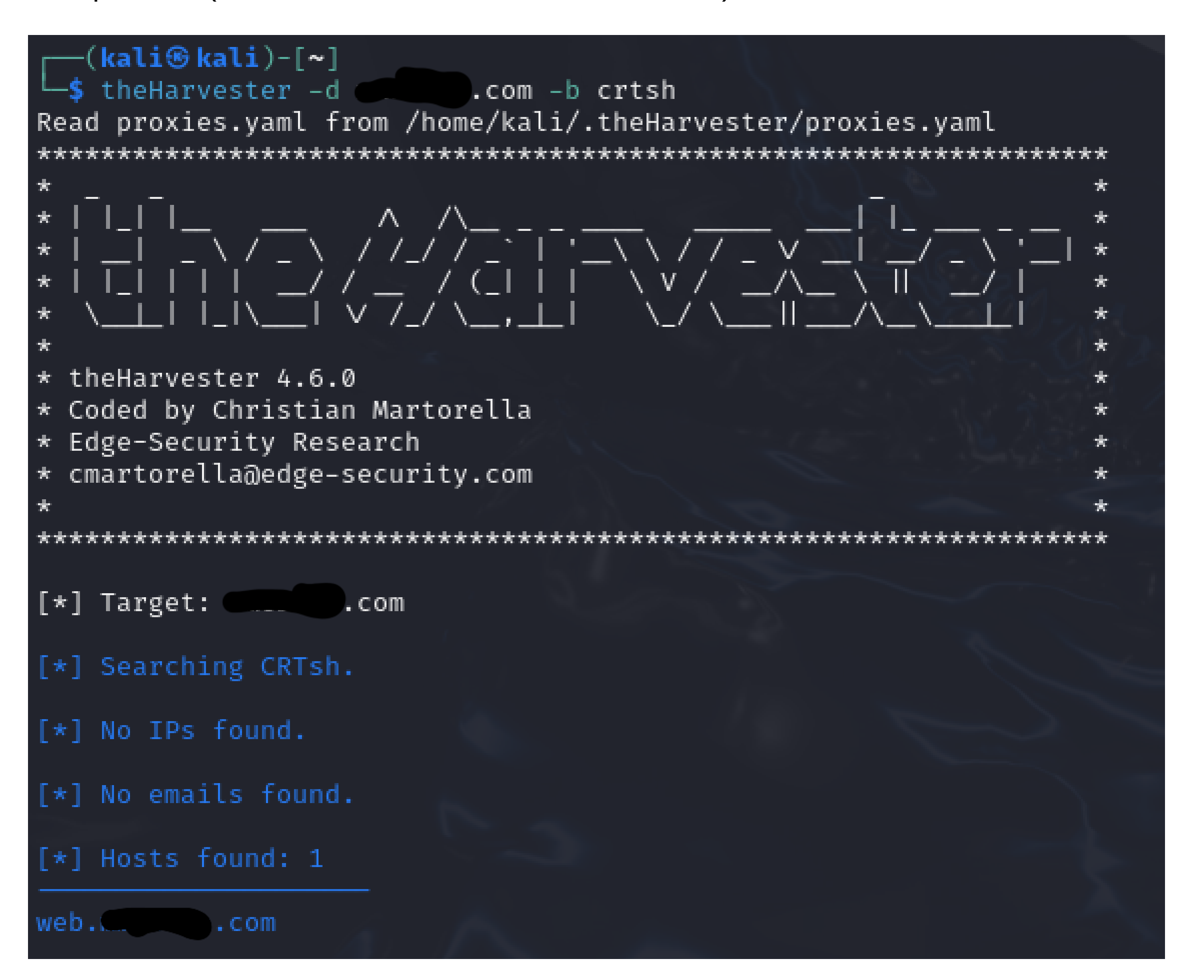
RubénS

```
[!] Missing API key for Tomba Key and/or Secret.
Read api-keys.yaml from /home/kali/.theHarvester/api-keys.yaml

[!] Missing API key for virustotal.
Read api-keys.yaml from /home/kali/.theHarvester/api-keys.yaml

[!] Missing API key for zoomeye.
[*] Searching Anubis.
        Searching 0 results.
[*] Searching Bing.
An exception has occurred: 400, message:
  Can not decode content-encoding: br
        Searching results.
[*] Searching Certspotter.
[*] Searching CRTsh.
An exception occurred: list index out of range
Unclosed client session
client_session: <aiohttp.client.ClientSession object at 0x7fa6e7524050>
[*] Searching Dnsdumpster.
[*] Searching Baidu.
[*] Searching Duckduckgo.
[*] Searching Otx.
[*] Searching Hackertarget.
An exception has occurred: 400, message:
  Can not decode content-encoding: br
Sitedossier module has triggered a captcha on first iteration, no results can be found.
Change IPs, manually solve the captcha, or wait before rerunning Sitedossier module
[*] Searching Sitedossier.
[*] Searching Rapiddns.
[*] Searching Subdomaincenter.
[*] Searching Subdomainfinderc99.
```

Más pruebas (encuentro un subdominio usando crtsh):

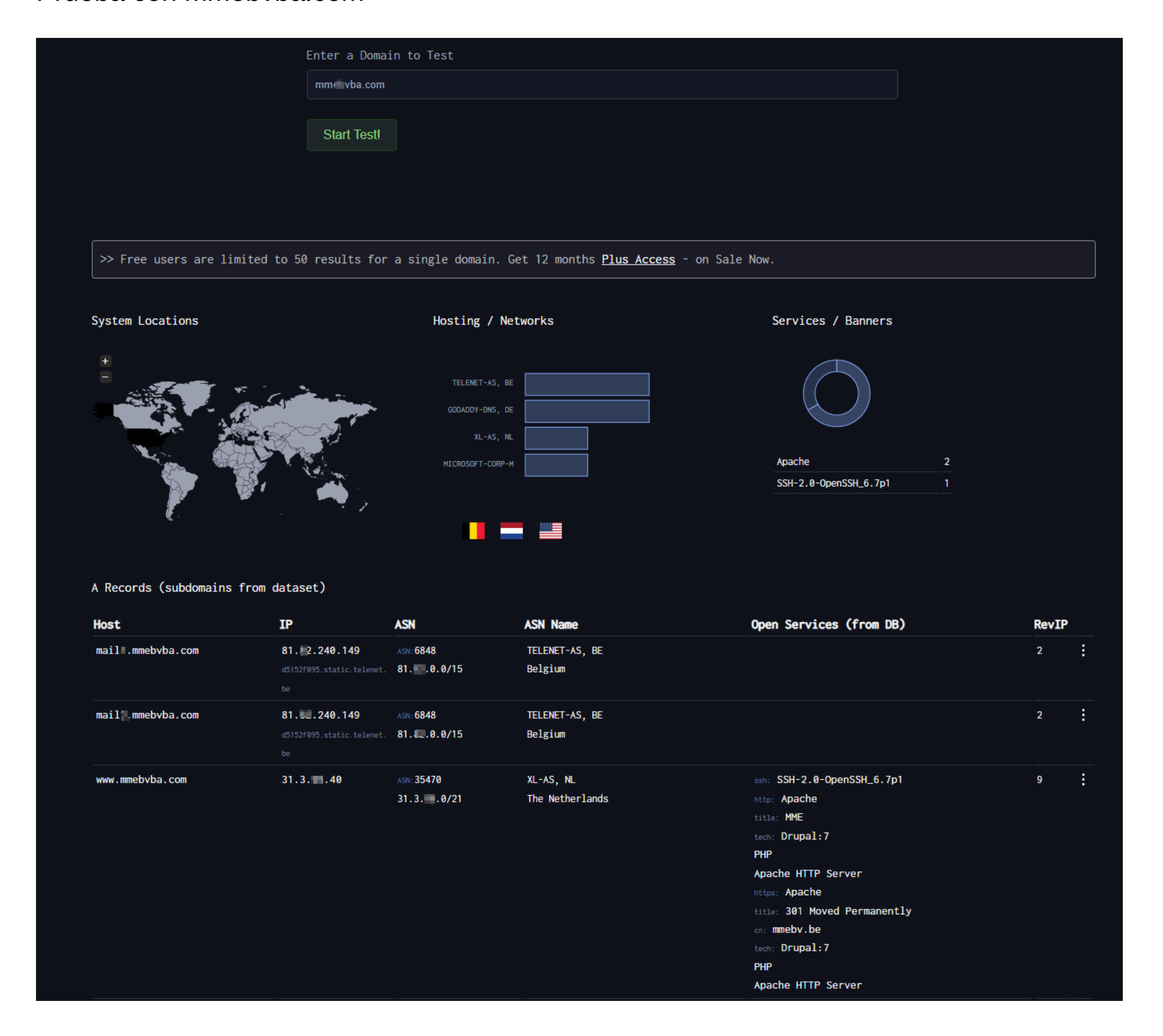


RubénS

5. Dnsdumpster

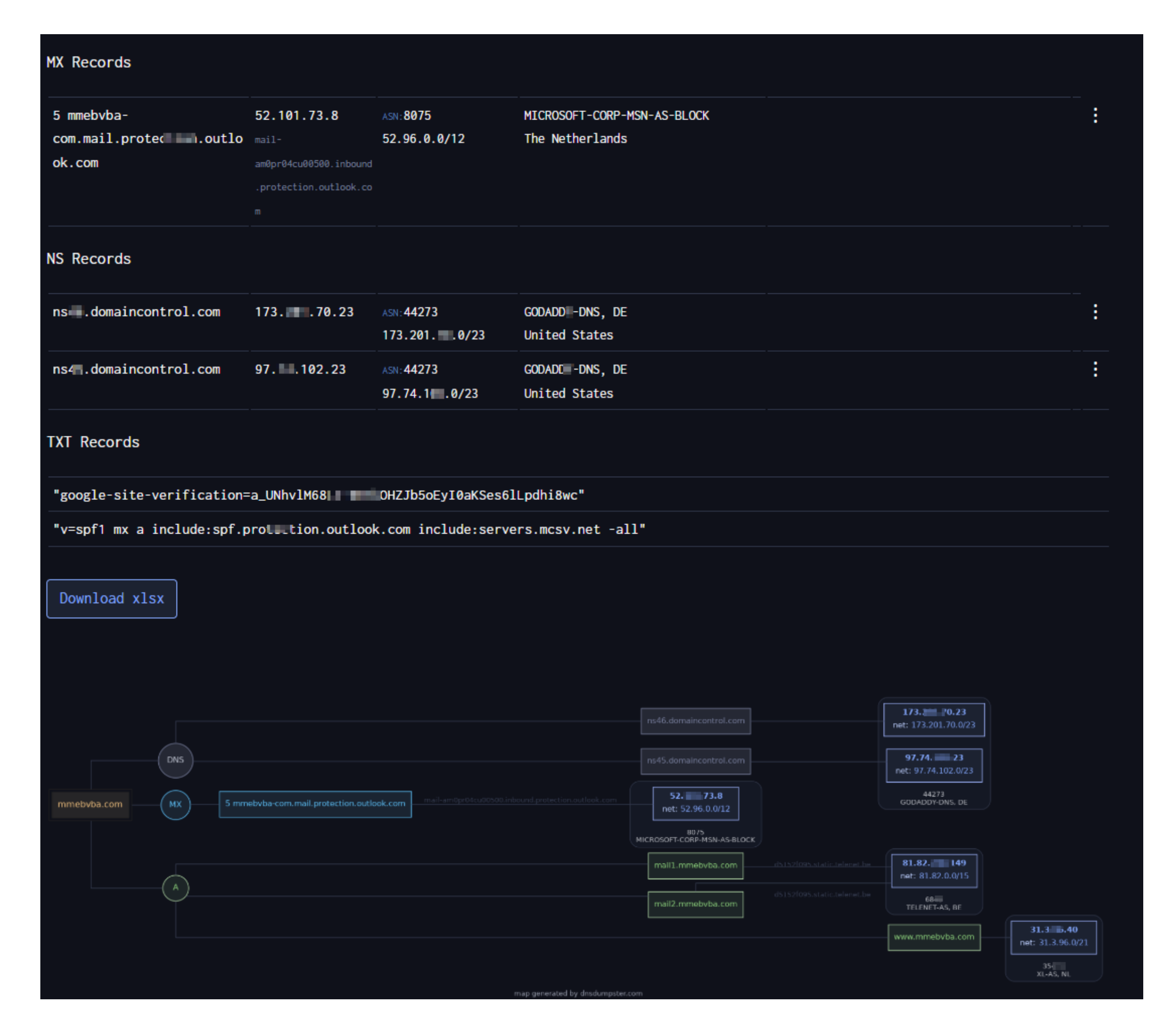
Una manera de obtener información sobre dominios es no hacerlo directamente sino a través de algún servicio online que ya se ha encargado de hacer esos reconocimientos dns.
En este caso usaremos el servicio https://dnsdumpster.com
De esta manera nuestra dirección IP no aparece directamente en los logs de los servidores dns, aunque sí en los logs del servidor de dnsdumpster. Esto es fácil de evitar si utilizamos alguna técnica de ocultación IP como la dark net (Tor, ZeroNet, I2P, etc) o una **VPN** (NordVPN, etc)
Utiliza dnsdumpster para obtener información de algún dominio (tiene que ser ahora un dominio real).

Prueba con mmebvba.com



Se pueden averiguar los proveedores de hosting, los servicios que usa (apache, ssh, drupal, php), subdominios y ubicaciones.

RubénS



Aquí se aprecian los registros de correo, proveedor de este, ubicación de este. Los servidores de nombres, ip, proveedor y ubicación.
Los TXT Records són los códigos de verificación de Google, y la de Outlook es para evitar spoofing en el correo. También usa MailChmp para márketing.
Lo siguiente es un mapa de la infraestructura DNS que muestra la relación entre registros DNS y servidores.

RubénS

Prueba con vulnweb.com:

Enter a Domain to Test

testphp.vulnweb.com

Start Test!

>> Free users are limited to 50 results for a single domain. Get 12 months Plus Access - on Sale Now.

S tem Locations

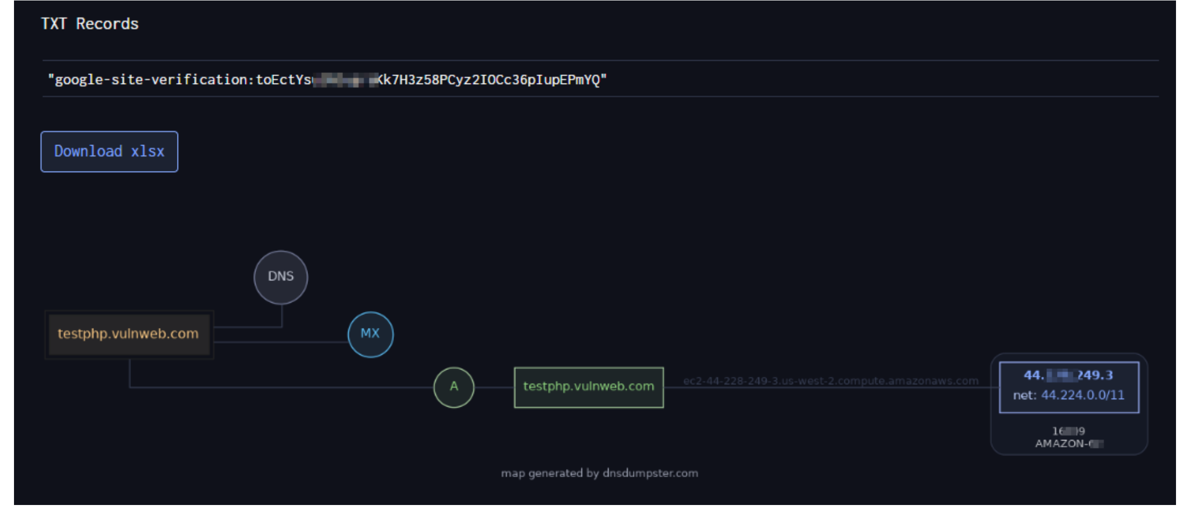
Hosting / Networks

Services / Banners

AMAZON-02

A Records (subdomains from dataset)

Host	IP	ASN	ASN Name	Open Services (from DB)	RevIP
testphp.vulnweb.com	44.228.249.3 ec2-44-228-249-3.us-west-2.compute.amazonaws.com	ASN:16509 44.224.0.0/11	AMAZON-02 United States		9



6. La herramienta **amass de OWASP** realiza el mapeo de la superficies de ataque y el descubrimiento de activos externos mediante la recopilación de información de código abierto y técnicas de reconocimiento activo. Amass utiliza fuentes de información como:

   DNS mediante técnicas de fuerza bruta, barridos de DNS inverso, transferencias de zona y permutaciones de nombres de subdominio, scraping de datos de motores de búsqueda y servicios como Ask, Baidu, Bing, DNSDumpster, DuckDuckGo, entre otros, análisis de registros de transparencia de certificados y fuentes como Censys, CertSpotter y Crt.sh, integración con APIs de servicios como AlienVault, BinaryEdge, BuiltWith, Shodan, VirusTotal, entre otros, consulta de archivos históricos en plataformas como Wayback Machine y Archive.today. Estas fuentes permiten a Amass obtener una visión detallada de la infraestructura online de una organización e identificar gracias a ello posibles vectores de ataque y activos expuestos.

   Tutorial de amass:
   https://github.com/OWASP/Amass/blob/master/doc/tutorial.md
   Aunque viene instalada de serie en Kali, es conveniente instalar la última versión desde github.

   Puedes bajar el binario para linux de 64 bits (amd64) en:
   https://github.com/OWASP/Amass/releases
   Voy a usar la última versión para Linux (**v4.1.0**).

   Amass incluye varios subcomandos que realizan diferentes acciones. Puedes consultar la ayuda con amass -h.

   Puedes consultar la ayuda completa en:
   https://github.com/OWASP/Amass/blob/master/doc/user_guide.md
   Realiza las siguientes consultas e indica qué es lo que realizan. Puedes consultar.

amass enum -v -src -ip -brute -d ceti.local

- amass enum: Ejecuta el subcomando enum, que se utiliza para realizar el descubrimiento de subdominios y mapear activos relacionados con un dominio.
- -v: Modo verbose, proporciona información detallada en la salida para que puedas ver el progreso y los detalles del escaneo.
- -src: Incluye las fuentes de donde se obtuvo la información (por ejemplo, APIs, bases de datos, y servicios web).
- -ip: Resuelve y muestra las direcciones IP asociadas a los subdominios encontrados.
- -brute: Realiza fuerza bruta para descubrir subdominios adicionales.
- -d ceti.local: Define el dominio objetivo (en este caso, ceti.local).

```
xubu@rubens:~/amass_Linux_amd64$ amass enum -v -src -ip -brute -d domirub.local
Querying URLScan for domirub.local subdomains
Querying Digitorus for domirub.local subdomains
Querying AlienVault for domirub.local subdomains
Querying Baidu for domirub.local subdomains
Querying UKWebArchive for domirub.local subdomains
Querying ArchiveIt for domirub.local subdomains
Querying Censys for domirub.local subdomains
Querying Gists for domirub.local subdomains
Querying HAW for domirub.local subdomains
Querying RapidDNS for domirub.local subdomains
Querying AbuseIPDB for domirub.local subdomains
Querying Arquivo for domirub.local subdomains
Querying AnubisDB for domirub.local subdomains
Querying PKey for domirub.local subdomains
Querying BufferOver for domirub.local subdomains
Querying DNSDumpster for domirub.local subdomains
Querying Searchcode for domirub.local subdomains
Querying SiteDossier for domirub.local subdomains
Querying CertSpotter for domirub.local subdomains
Querying Wayback for domirub.local subdomains
Querying ThreatCrowd for domirub.local subdomains
Querying HyperStat for domirub.local subdomains
Querying Maltiverse for domirub.local subdomains
Querying Greynoise for domirub.local subdomains
Querying Searx for domirub.local subdomains
Querying Sublist3rAPI for domirub.local subdomains
Querying Bing for domirub.local subdomains
Querying GoogleCT for domirub.local subdomains
Querying HackerOne for domirub.local subdomains
Querying Mnemonic for domirub.local subdomains
Querying Crtsh for domirub.local subdomains
Querying Riddler for domirub.local subdomains
Querying FullHunt for domirub.local subdomains
Querying IPv4Info for domirub.local subdomains
Querying Ask for domirub.local subdomains
Querying Brute Forcing for domirub.local subdomains
Querying DuckDuckGo for domirub.local subdomains
Querying SonarSearch for domirub.local subdomains
Querying Robtex for domirub.local subdomains
Querying N45HT for domirub.local subdomains
Querying ThreatMiner for domirub.local subdomains
Querying CommonCrawl for domirub.local subdomains
Querying HackerTarget for domirub.local subdomains
Querying Yahoo for domirub.local subdomains
No names were discovered

The enumeration has finished
Discoveries are being migrated into the local database
```

En este caso esta información no es útil, ya que Amass requiere acceso a información de fuentes públicas y, en un dominio local o interno, esta información no estará disponible.
Para entornos internos, herramientas como Nmap o DNS internos pueden ser más efectivas.

Probando con vulnweb:

```
┌──(kali㉿kali)-[~]
└─$ amass enum -v -brute -d testphp.vulnweb.com
Querying DNSHistory for testphp.vulnweb.com subdomains
Querying Bing for testphp.vulnweb.com subdomains
Querying Searchcode for testphp.vulnweb.com subdomains
Querying Sublist3rAPI for testphp.vulnweb.com subdomains
Querying Synapsint for testphp.vulnweb.com subdomains
Querying LeakIX for testphp.vulnweb.com subdomains
Querying Riddler for testphp.vulnweb.com subdomains
Querying URLScan for testphp.vulnweb.com subdomains
Querying Ask for testphp.vulnweb.com subdomains
Querying DNSSpy for testphp.vulnweb.com subdomains
Querying Google for testphp.vulnweb.com subdomains
Querying HyperStat for testphp.vulnweb.com subdomains
Querying Crtsh for testphp.vulnweb.com subdomains
Querying CertSpotter for testphp.vulnweb.com subdomains
Querying Mnemonic for testphp.vulnweb.com subdomains
Querying AbuseIPDB for testphp.vulnweb.com subdomains
Querying Baidu for testphp.vulnweb.com subdomains
Querying CommonCrawl for testphp.vulnweb.com subdomains
Querying DNS SRV for testphp.vulnweb.com subdomains
Querying PKey for testphp.vulnweb.com subdomains
Querying SubdomainCenter for testphp.vulnweb.com subdomains
Querying Yahoo for testphp.vulnweb.com subdomains
Querying Arquivo for testphp.vulnweb.com subdomains
Querying HAW for testphp.vulnweb.com subdomains
Querying Gists for testphp.vulnweb.com subdomains
Querying SiteDossier for testphp.vulnweb.com subdomains
Querying Digitorus for testphp.vulnweb.com subdomains
Querying Active Crawl for testphp.vulnweb.com subdomains
Querying Active DNS for testphp.vulnweb.com subdomains
Querying AnubisDB for testphp.vulnweb.com subdomains
Querying GrepApp for testphp.vulnweb.com subdomains
Querying Wayback for testphp.vulnweb.com subdomains
Querying HackerTarget for testphp.vulnweb.com subdomains
Querying RapidDNS for testphp.vulnweb.com subdomains
Querying Searx for testphp.vulnweb.com subdomains
Querying ThreatMiner for testphp.vulnweb.com subdomains
Querying UKWebArchive for testphp.vulnweb.com subdomains
Querying DNSDumpster for testphp.vulnweb.com subdomains
Querying Maltiverse for testphp.vulnweb.com subdomains
Querying Pulsedive for testphp.vulnweb.com subdomains
Querying DuckDuckGo for testphp.vulnweb.com subdomains
Querying Greynoise for testphp.vulnweb.com subdomains
Querying HackerOne for testphp.vulnweb.com subdomains
Querying AlienVault for testphp.vulnweb.com subdomains
Querying Brute Forcing for testphp.vulnweb.com subdomains
testphp.vulnweb.com (FQDN) ⟶ a_record ⟶ 44.228.249.3 (IPAddress)
44.224.0.0/11 (Netblock) ⟶ contains ⟶ 44.228.249.3 (IPAddress)
16509 (ASN) ⟶ managed_by ⟶ AMAZON-02 - Amazon.com, Inc. (RIROrganization)
16509 (ASN) ⟶ announces ⟶ 44.224.0.0/11 (Netblock)

The enumeration has finished
```

El dominio está alojado en los servidores de Amazon Web Services (AWS). Esto puede ser relevante para investigar configuraciones específicas de la nube (por ejemplo, servicios mal configurados).

```
e.com (FQDN) ⟶ mx_record ⟶ alt3.aspmx.l.google.com (FQDN)
e.com (FQDN) ⟶ mx_record ⟶ al[redacted]spmx.l.google.com (FQDN)
e.com (FQDN) ⟶ mx_record ⟶ alt2.aspmx.l.google.com (FQDN)
e.com (FQDN) ⟶ mx_record ⟶ alt4.aspmx.l.google.com (FQDN)
e.com (FQDN) ⟶ mx_record ⟶ aspmx.l.google.com (FQDN)
```

Gracias a este reconocimiento pasivo, estos registros indican que xxxx utiliza Google como proveedor de servicios de correo. Esto puede ser útil para realizar pruebas relacionadas con phishing o spoofing (simulando correos falsos).

```
┌──(kali㉿kali)-[~]
└─$ amass enum -v -brute -d [redacted]a.com
```

```
.com (FQDN) ⟶ mx_record ⟶ [redacted]-com.mail.protect[redacted].outlook.com (FQDN)
.com (FQDN) ⟶ ns_record ⟶ ns46.doma[redacted]control.com (FQDN)
.com (FQDN) ⟶ ns_record ⟶ ns45.domai[redacted]control.com (FQDN)
```

La primera línea indica que el correo del dominio se gestiona a través del servicio de protección de correo de Outlook (Microsoft).
Y los siguientes apuntan a los servidores de nombres.

Ahora pruebo el commando:

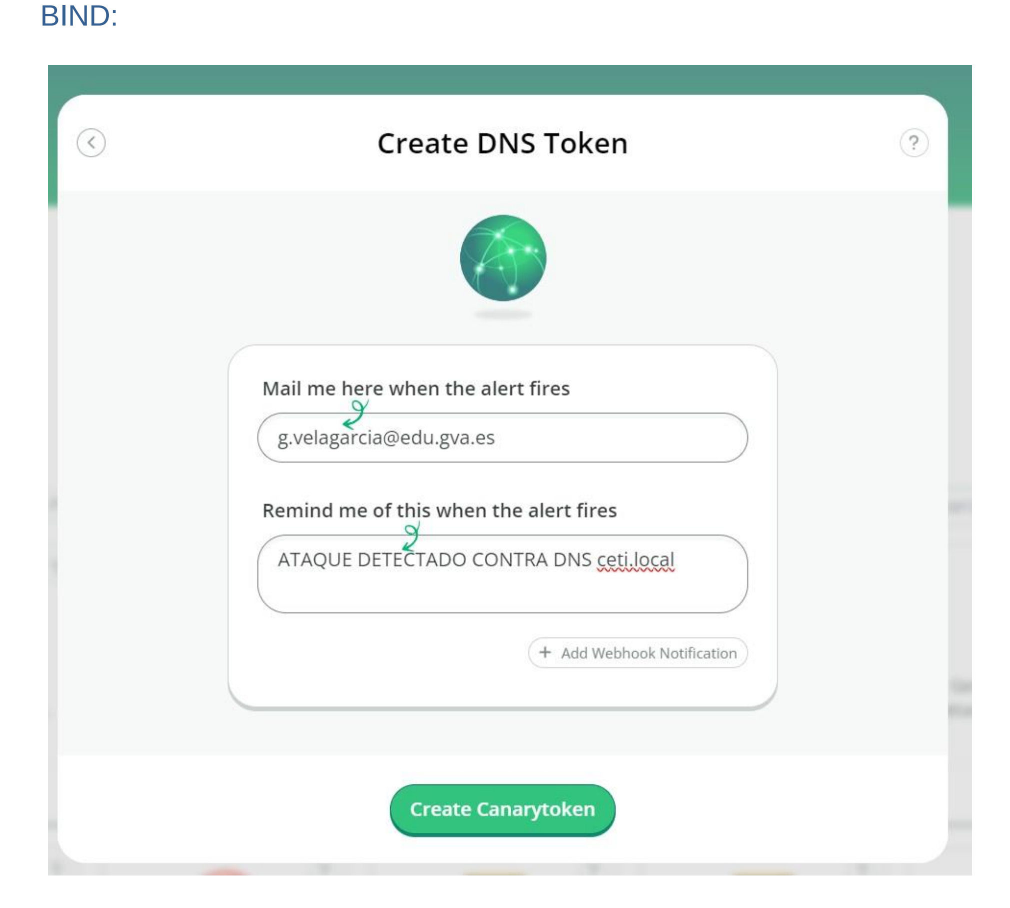
amass intel -v -whois -src -ip -d ceti.local

- amass intel: Ejecuta el subcomando intel, que está diseñado para recopilar inteligencia sobre posibles dominios y activos relacionados.
- -v: Modo verbose, muestra información detallada en la salida para que puedas monitorear el progreso y resultados.
- -whois: Incluye búsquedas en bases de datos WHOIS para identificar dominios relacionados con el dominio objetivo.
- -src: Muestra las fuentes de información utilizadas para la recopilación de datos.
- -ip: Incluye la resolución de direcciones IP relacionadas con los dominios o subdominios encontrados.
- -d ceti.local: Especifica el dominio objetivo para el análisis (en este caso, ceti.local).

Aquí digo lo mismo que antes, este comando es más útil para dominios públicos y reales, donde la consulta WHOIS y las fuentes de información pública pueden tener datos con algún valor.

7. Detección del ataque

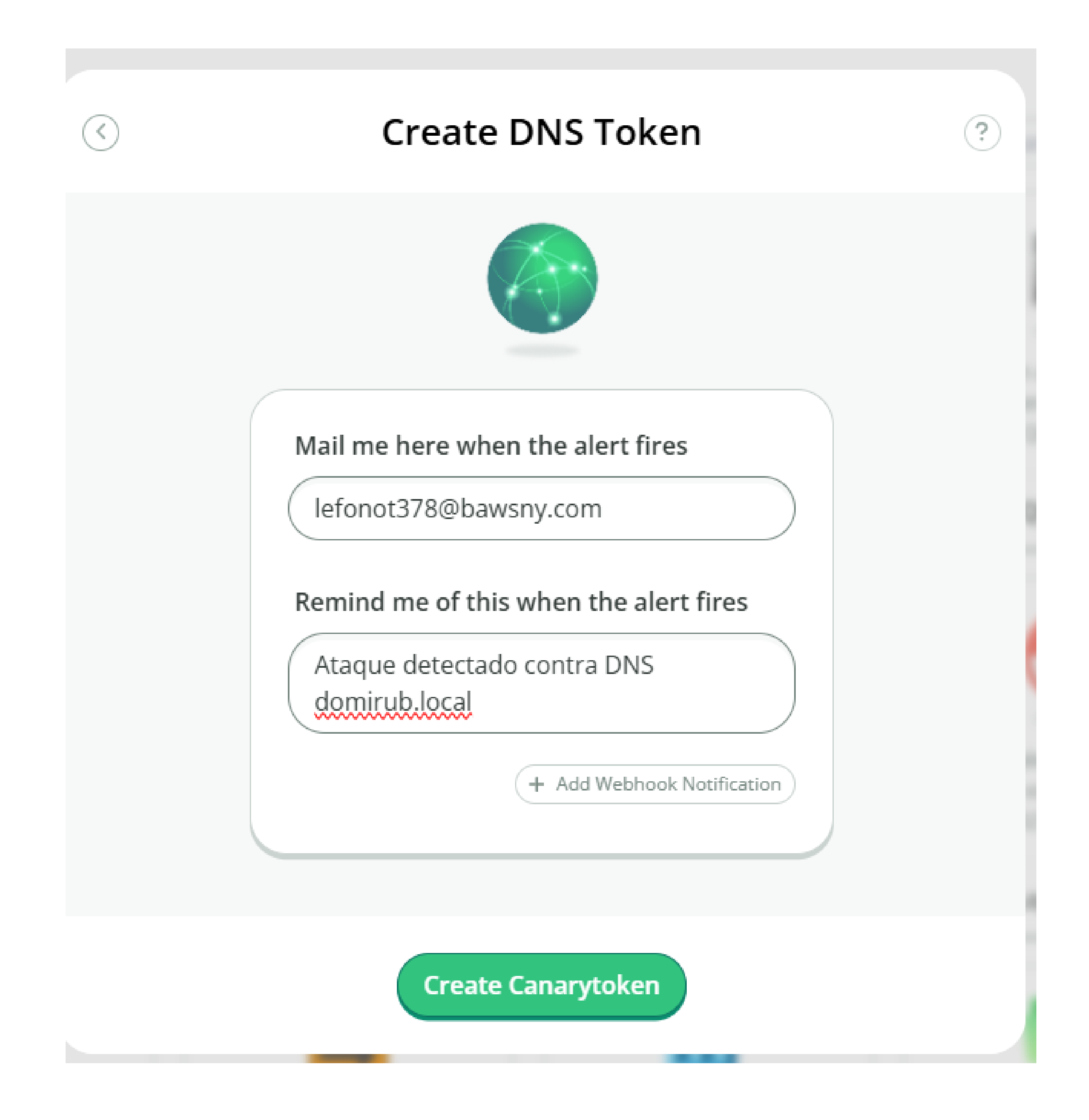
Un posible mecanismo de detección es dejar registros falsos en nuestro DNS para comprobar que si alguien lo solicita, es porque están haciendo un ataque de fuerza bruta contra nuestro DNS.
Los honeypots son sistemas a modo de señuelos que sirven para comprobar las técnicas de ataque de los ciberdelincuentes. Un servicio online de honeypots es https://canarytokens.org.
Accede a dicho servicio y crear un canario de tipo DNS.
Configura ahora tu dns para que tenga un registro CNAME que apunte al nombre DNS que te genera el canario una vez le das a Create my CanaryToken,
BIND:



windows IN CNAME rehro47bpl57fefns24sv6.canarytokens.com.

Cuando alguien pida la máquina windows (que es un señuelo en nuestra zona DNS) y resuelva el nombre posterior canónico al que apunta el registro, se nos enviará una alerta por email
Una vez configurado el señuelo en tu dominio, lanza un ataque de enumeración (o que lo hagaun compañero simulando un atacante) contra tu dominio para comprobar el funcionamiento del canario.
Realiza capturas de todo el proceso: creación canario, configuración y alerta recibida.

RubénS



Token generado:

c5dnojvcqyqu7exzf8uhp27p7.canarytokens.com

Añado esta línea a /etc/bind/zones/db.domirub.local

```
 GNU nano 8.1                /etc/bind/db.domirub.local
$TTL 604800
@ IN SOA domirub.local. root.domirub.local. (
    2024010100 ; Serial
    604800     ; Refresh
    86400      ; Retry
    2419200    ; Expire
    604800 )   ; Negative Cache TTL
;
@ IN NS ns1.domirub.local.
@ IN A 192.168.0.1

ns1     IN A 192.168.0.1
web     IN A 192.168.0.10
mail    IN A 192.168.0.20
ftp     IN A 192.168.0.30
windows IN CNAME c5dnojvcqyqu7exzf8uhp27p7.canarytokens.com.
```

Compruebo que el archivo está bien:

```
xubu@rubens:~$ named-checkzone domirub.local /etc/bind/db.domirub.local
zone domirub.local/IN: loaded serial 2024010100
OK
```

Guardo los cambios y reinicio bind9 con sudo systemctl restart bind9.

Esto no funcionará sin que tu servidor DNS pueda reenviar consultas al exterior, ya que se neceista que las consultas DNS lleguen hasta sus servidores en Internet. Sin acceso a Internet, dichas consultas nunca podrán ser resueltas por el servicio de canarytokens, por lo que no se generarán alertas.

Para tratar de solucionar esto voy a configura en named.conf.options un forwarder que reenvíe las consultas desconocidas a un servidor DNS con acceso a Internet.

```
  GNU nano 8.1              /etc/bind/named.conf.options *
// named.conf.options
options {
    directory "/var/cache/bind";
    recursion yes;
    allow-query { any; };
    forwarders {
        8.8.8.8;
        8.8.4.4;
    };
    dnssec-validation auto;
};
```

```
xubu@rubens:~$ dig @127.0.0.1 windows.domirub.local

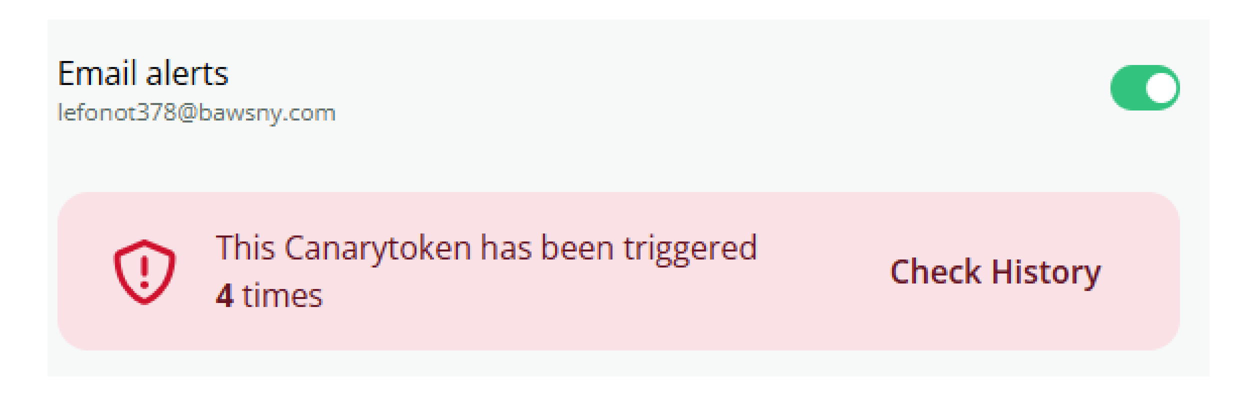
; <<>> DiG 9.20.0-2ubuntu3-Ubuntu <<>> @127.0.0.1 windows.domirub.local
; (1 server found)
;; global options: +cmd
;; Got answer:
;; WARNING: .local is reserved for Multicast DNS
;; You are currently testing what happens when an mDNS query is leaked to DNS
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 49523
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 2, AUTHORITY: 0, ADDITIONAL: 1

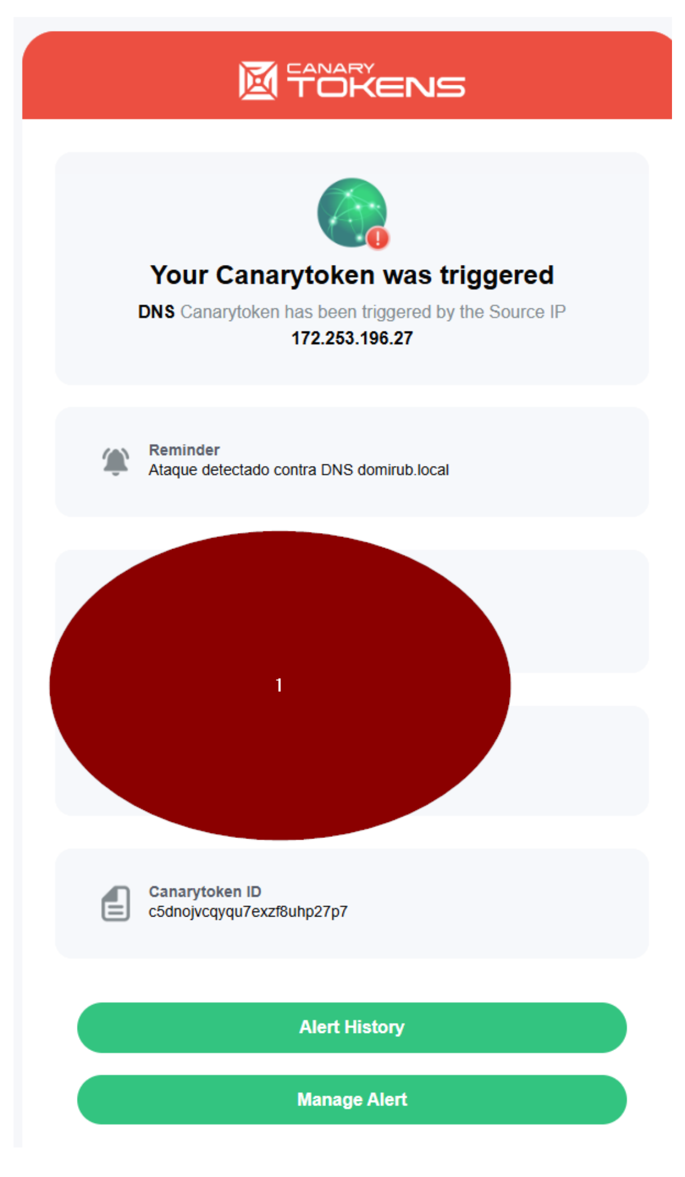
;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 1232
; COOKIE: eac3c2dcd7133b330100000067563916bb2c27e870316fb0 (good)
;; QUESTION SECTION:
;windows.domirub.local.         IN      A

;; ANSWER SECTION:
windows.domirub.local.  604800  IN      CNAME   c5dnojvcqyqu7exzf8uhp27p7.canarytok
ens.com.
c5dnojvcqyqu7exzf8uhp27p7.canarytokens.com. 10 IN A 52.18.63.80

;; Query time: 667 msec
;; SERVER: 127.0.0.1#53(127.0.0.1) (UDP)
;; WHEN: Mon Dec 09 01:25:58 CET 2024
;; MSG SIZE  rcvd: 150
```

Si alguien solicita el registro windows.domirub.local, el servidor DNS intentará resolver el nombre canónico al que apunta el CNAME, activando el CanaryToken.





Alerts History



DNS Canarytoken ID: **c5dnojvcqyqu7exzf8uhp27p7**

